APPLICANT RESPONSE TO NON COMPLIANT ACTION

Inventor Nick Nassiri (hereinafter referred to as the "Applicant") is in receipt of the Examiner's Action dated November 02, 2005 with respect to the above named patent application. Applicant wishes to address each of the Examiner's objections as put forth in the Non-Compliant Action.

SPECIFICATION

Examiner states that the substituted specification contains new matter, and should properly be filed as a CIP. Applicant has amended the original specification again to comport with Examiner's concerns. Accordingly, Applicant respectfully requests that Examiner withdraw his objection in lieu of the attached substitute specification.

Applicant agrees with Examiner that the substitute specification is rife with deletions; however, Applicant submits that deletions do not constitute new matter.

Applicant respectfully notes that the Examiner has failed to specify what constitutes new matter in the substituted specification. Applicant submits that no new matter has been presented in the substitute specification, as amended herein; rather Applicant has clarified a poorly written specification by <u>clarifying original material contained in the original disclosure.</u> Applicant is aware that the substitute specification is a confusing read, and has revised the substitute

Application Number 09/973, 273

specification in accordance with the guidelines of CFR § 1.121 (b).[1] Applicant

respectfully submits that the code, as cited by the Examiner, does not prohibit

---

[1] Specification. Amendments to the specification, other than the claims,

computer listings (§ 1.96) and sequence listings (§ 1.825), must be

made by adding, deleting or replacing a paragraph, by replacing a

section, or by a substitute specification, in the manner specified in

this section.

(1) Amendment to delete, replace, or add a paragraph. Amendments to the
specification, including amendment to a section heading or the title of
the invention which are considered for amendment purposes to be an
amendment of a paragraph, must be made by submitting:

(i) An instruction, which unambiguously identifies the location, to
delete one or more paragraphs of the specification, replace a paragraph
with one or more replacement paragraphs, or add one or more paragraphs;

(ii) The full text of any replacement paragraph with markings to show
all the changes relative to the previous version of the paragraph. The
text of any added subject matter must be shown by underlining the added
text. The text of any deleted matter must be shown by strike-through
except that double brackets placed before and after the deleted
characters may be used to show deletion of five or fewer consecutive
characters. The text of any deleted subject matter must be shown by
being placed within double brackets if strike-through cannot be easily
perceived;

(iii) The full text of any added paragraphs without any underlining;
and

(iv) The text of a paragraph to be deleted must not be presented with
strike-through or placed within double brackets. The instruction to
delete may identify a paragraph by its paragraph number or include a
few words from the beginning, and end, of the paragraph, if needed for
paragraph identification purposes.

(2) Amendment by replacement section. If the sections of the
specification contain section headings as provided in § 1.77(b), §
1.154(b), or § 1.163(c), amendments to the specification, other than
the claims, may be made by submitting:

(i) A reference to the section heading along with an instruction,
which unambiguously identifies the location, to delete that section of

- 2 -

Application Number 09/973, 273

deletions or revisions to the specification, so long as said revisions contain no

new matter and are in compliance with CFR § 1.121 (b) .

Applicant respectfully submits the revised substitute specification comports with

CFR § 1.121 (b)); clearly identifying the deletions and revisions for the

Examiner's review vis-à-vis the original specification.

---

the specification and to replace such deleted section with a
replacement section; and

(ii) A replacement section with markings to show all changes relative
to the previous version of the section. The text of any added subject
matter must be shown by underlining the added text. The text of any
deleted matter must be shown by strike-through except that double
brackets placed before and after the deleted characters may be used to
show deletion of five or fewer consecutive characters. The text of any
deleted subject matter must be shown by being placed within double
brackets if strike-through cannot be easily perceived.

(3) Amendment by substitute specification. The specification, other
than the claims, may also be amended by submitting:

(i) An instruction to replace the specification; and

(ii) A substitute specification in compliance with § § 1.125(b) and
(c).

(4) Reinstatement of previously deleted paragraph or section. A
previously deleted paragraph or section may be reinstated only by a
subsequent amendment adding the previously deleted paragraph or
section.

INSTRUCTIONS FOR AMENDMENT OF THE ORIGINAL

SPECIFICATION

1. Applicant respectfully requests that the enclosed amended specification replace the existing original specification on file and the substitute specification on file in its entirety.

2. Applicant requests that paragraphs 16-20 of the original specification be deleted in their entirety and replaced with the following text:

    The main problem with conventional real-time, live-stream videoconferencing methods is that none of the existing systems or applications incorporate a system, method or process, whereby an identity, or a signature, or the contents of a document is verified during the videoconference.

    Another problem with conventional real-time, live-stream videoconferencing methods is that none of the existing systems or applications incorporate a system, method or process whereby biometric data is input during the videoconference to verify an

identity, or a signature, or the contents of a document.

Another problem with conventional real-time, live-stream videoconferencing methods is that none of the existing systems or applications incorporate a system, method or process whereby a signature may be notarized by a notary public during the videoconference.

Another problem with conventional real-time, live-stream videoconferencing methods is that none of the existing systems or applications incorporate a system, method or process whereby a client may tender a service request for videoconference verification from a remote location using the Internet.

Another problem with conventional real-time, live-stream videoconferencing methods is that none of the existing systems or applications incorporate a system, method or process whereby an authoritative document is created and issued during the videoconference.

3. Applicant requests that paragraph 23 of the original specification be deleted in its entirety and replaced with the following text:

The general purpose of the present invention, which will be described subsequently in greater detail, is to provide a new method of a real- time, live-stream-video-conference wherein a client may request verification of an identity (identity being an individual), a signature (signature belonging to an individual), or the contents of a document (document being either hard-copy or electronic), and whereby an authoritative document is created (the authoritative document ("A.D.") is either a hard copy document or electronic record or both).

4.   Applicant requests that paragraphs 62-64 of the original specification be deleted in their entirety and replaced with the following text:

FIG. 1 discloses a method for identity verification. The distinction between the "public" and "private" domain is whether the service request involves a government/regulatory entity (Governmental Agency/ G.A.) or a private party (Private). The former designation being deemed a "public" process whereby the signature or identity authentication is for the purpose of creating a government or a regulatory based identity document. The latter designation being deemed a "private" process whereby identity authentication is for the purpose of a commercial transaction.

FIG. 1A discloses the method of identity criteria input by a customer.

FIG. 2 discloses the method of a public client service request for signature verification utilizing a notary public, if necessary, and whereby the VVSC downloads a document from the VVSC electronic document repository.

FIG. 2A discloses the method of a private client service request for signature verification utilizing a notary public, if necessary, and whereby the VVSC downloads a document from the VVSC electronic document repository.

FIG. 2B discloses the method of a public client service request for signature verification utilizing a notary public, if necessary and whereby the VVSC uploads a document into the VVSC electronic document repository to enable the service request.

FIG. 2C discloses the method of a private client service request for signature verification utilizing a notary public, if necessary, and whereby the VVSC uploads a document into the VVSC electronic document repository to enable the service request.

FIG. 3 discloses the method of a private client service request for identity, or signature, or document verification utilizing the VVSC website.

FIG. 3A discloses the method of a public client service request for identity, or signature, or document verification utilizing the VVSC website.

FIG. 3B discloses the method of a private client service request for signature verification utilizing a notary public, if necessary, via the VVSC website, and whereby the client downloads a document from the VVSC electronic document repository to enable the service request.

FIG. 3C discloses the method of a private client service request for signature verification utilizing a notary public, if necessary, via the VVSC website, and whereby the client uploads a document into the VVSC electronic document repository to enable the service request.

FIG. 3D discloses the method of a private client registration request to use the services offered via the VVSC website, and

whereby the client inputs the identity criteria to establish the client registration account.

FIG. 3E discloses the method of a public client registration request to use the services offered via the VVSC website, and whereby the client inputs the identity criteria to establish the client registration account.

5. Applicant requests that paragraphs 178-184 of the original specification be deleted in their entirety and replaced with the following text:

Video Verification Service Center (VVSC)

The VVSC is a physical structure, a place of business, where either a client or a customer can go to process a service request, The VVSC is staffed by VVSC employees and is equipped with the infrastructure to enable the service requests, as disclosed herein. The VVSC enables the service request tendered by the client and coordinates the schedule of the parties to the videoconference.

The VVSC establishes the time and date and locations for the real-time, live-stream videoconference between the client and customer(s). All parties to the videoconference receive a confirmation prior to the videoconference via electronic mail or

other forms of messaging, such as text, or mail or telephone,

informing said parties of the time, date and location of the

videoconference. The parties are advised of the contents of the

service request, and the necessary identity criteria that must be

provided during the videoconference. The VVSC enables and

manages the services requested by the client; irrespective of the

different location of the client and customer. The VVSC provides

the necessary infrastructure and applications for the

videoconference, the service request, and to create the finalized

authoritative document.

Video Verification Service Center Website (VVSC website)

In the preferred embodiment, the VVSC website is accessible via

the Internet. The VVSC website provides the service requests

disclosed herein: identity, or signature, or document verification.

The VVSC website enables a client or a customer to access

authentication services from a local computer system (e.g. their

home or office), without having to physically visit a VVSC.

The VVSC website establishes the time and date and locations for

the real-time, live-stream videoconference between the client and

customer(s). All parties to the videoconference receive a

confirmation prior to the videoconference via electronic mail or

other forms of messaging, such as text, or mail or telephone,

informing said parties of the time, date and location of the

videoconference. The parties are advised of the contents of the

service request, and the necessary identity criteria that must be

provided during the website videoconference. The VVSC enables

and manages the services requested by the client; irrespective of

the different location of the client and customer. The VVSC

provides the necessary infrastructure and applications for the

website videoconference, the service request, and to create the

finalized authoritative document.

Service Request or Request for Services

A service request, or request for services; used interchangeably,

mean a request from a client for any of the foregoing services from

the VVSC or the VVSC website. Specifically: identity verification, or

signature verification, or document verification, or any combination

thereof. Irrespective of the client's service request, it is processed

in the context of a real-time, live-stream videoconference. A client

may tender a single service request, or multiple service requests, to

be fulfilled in the course of the videoconference.

Client and Customer

A client is the individual tendering the service request to the VVSC
or the VVSC website. A customer is the individual whose identity,
or signature, or documents are being verified. In some transactions,
a client may also request that the client's identity, or client's
signature, or client's document be authenticated during the
videoconference, along with the customer's. By way of example, a
client and a customer may wish to verify the identity and signature
of one another to conclude a commercial transaction, such as the
purchase of real estate, during the videoconference. In this
instance, each party would input identifying criteria to be
authenticated by the VVSC. It is to be understood that there may be
multiple clients, or customers involved in a single videoconference.
Collectively, the group of individuals participating in the
videoconference are referred to as "the Parties".

Governmental Agency (Public) and Private Party (Private)
A distinction is made between the type of client tendering a service
request. A public client is deemed to be a governmental agency
(G.A.) such as the D.M.V. or the USPS, and a private party is
deemed to be an individual or business from the private sector.

Identifying Criteria or I.D. Criteria

Identifying criteria, or I.D. criteria; used interchangeably, comprise the data input that was used to authenticate either an identity, a signature, or a document. Likewise, identifying criteria is used to create the authoritative document. The identifying criteria for an individual is at least one of a group of: a signature, a fingerprint, a retina scan, a voiceprint, a hard copy identity document, a photograph, or a password/ code. Depending on the service request, a client may select any combination of the I.D. criteria to authenticate the customer, and any combination of the I.D. criteria to create the authoritative document. The identifying criteria of a public entity include at least one of a group of a hard-copy identity document 46, a password/ code 49, a signature 50, proof of executive identity/authority, a corporation number 232, or a photograph 52.

Verification or Authentication

Verification, or authentication (and variations on the verb thereof), are used interchangeably, and mean the process whereby either an identity, or a signature, or a document is verified (or authenticated) in accordance with the client's service request.

Authoritative Document (A.D.)

The authoritative document contains the identity criteria

information requested by the client in the service request.

Depending on the service request, the resulting authoritative

document is comprised of at least one of the following group: a

signature, a fingerprint, a retina scan, a voiceprint, a hard copy

identity document, a photograph, or a password/ code. The

authoritative document is created during the real-time, live-stream

videoconference. The authoritative document is issued during the

real-time, live-stream videoconference. In the preferred

embodiment, the authoritative document is issued in the form of an

identity card such as a passport or drivers license. The authoritative

document can also be issued as an electronic document or

electronic code that is stored in a hardware device, such as a disc

or chip. Regardless of the form of the authoritative document, each

authoritative document is encrypted with the I.D. criteria input and

secured with a time and date stamp.

Videoconference or Webconference

The term videoconference or webconference means a real-time,

live-stream video-communication between the parties . The present

invention may use various videoconference technologies and

applications thereof, but all are premised on the fact that it is a real

time, live stream transaction between the parties that are remote in location. The videoconference enables the exchange of visual and audio communication between the parties, in addition to enabling the transaction of the service request.

Document

An electronic document is used in the method of the present invention. The function of the electronic document repository is to fulfill the client service request. The electronic document may comprise audio, video, graphic, biometric, or text data. A client may elect to download an electronic document from an electronic document repository maintained by the present invention. Alternatively, a client may elect to upload an electronic document to enable the client service request. The VVSC electronic document repository contains a library of electronic documents typically used in public and private party transactions: Oaths, promissory notes, deeds, etc.. It is to be understood, that reference to a document means an electronic document, except where qualified as a hard copy document.

Electronic Signature Capture Device

An electronic signature capture device is used in the method of the present invention. The electronic signature capture device captures

the electronic signatures of the parties to the transaction. The electronic signature capture device is capable of assigning digital code, or a graphic image, or both to the authoritative document. The graphical representation depicts the actual hand-written signature of the signatory.

Signature

The term signature shall be construed to mean any form of electronic signature, including at least one of the group of a graphical, hand written representation, a digital certificate, a password, or other electronic data input qualified to constitute a signature.

Notary Public and Notarization

The term notary public and notarization means the process of authenticating a electronic document by a live, human-being commissioned notary public. The notary public notarizes the document in accordance with the law.

Electronic Notary Device

An electronic notary device is used for the method of the present invention. The electronic notary device provides a method of electronic notarization to verify a signature or an individual or the

contents of a document. An electronic notary stamp is affixed to a document in one of two ways: by manually imprinting the notary seal using the electronic signature capture device pad, or, alternatively, by utilizing an electronic device that is encrypted with the equivalent of the notary's stamp in the form of source code which embeds the notary code in the authoritative document.

6. Applicant requests that the Abstract of the original specification be deleted in its entirety and replaced with the following abstract:

The method of the present invention uses a real-time, live-stream videoconference to unite remote parties needing to verify either an identity, or a signature, or a document. During the videoconference, the method of the present invention verifies an individual's identity, or a signature, or a document by requesting data input from at least one of the parties to the videoconference. Said data input includes at least one of the group of a signature, a fingerprint, a retina scan, a voice print, a photograph, an identity document, or a password / code. Upon completion of the verification request, the method of the present invention creates an authoritative document, containing the data input, and issues it to a designated party. The authoritative document is created during the videoconference and is issued to the designated party before the videoconference terminates.

CLAIMS

Applicant presents the claims with the current status of each claim (as amended in Applicant's response to the First Office Action) identified.

Claims 1-4, 8-28, 30-56, 59-74 are pending.

Claims 6, 7, 29, 57, 58, 75, 76, and 77 are canceled.

Claim 78 is new.

DRAWINGS

Examiner objects to the drawings because they contain new matter. Applicant respectfully traverses. Applicant notes that the Examiner has failed to specify what new matter the replacement drawings contain. Per the Examiner's instruction, Applicant has provided herein an explanation pointing out how the replacement drawings are supported by the original disclosure, and the original drawings. Applicant has further numbered the original drawings as disclosed in the original specification, to show the continuity in the replacement drawings . Applicant submits that the original drawings failed to fully depict the claimed invention, as disclosed in the original specification, and that the replacement drawings fully depict the claimed invention in the original specification.

With respect to FIG 1 (Identity Verification Services/Overview), Applicant refers to the original specification in its entirety.

With respect to FIG 1A (Identification Criteria), Applicant refers to paragraph 76 through 79, and paragraph 91, and paragraph 93 of the original specification.

With respect to FIG 2 (Verification Using a Notary), Applicant refers to paragraph 72 through 84 and paragraphs 88 through 93, of the original specification.

With respect to FIG 2A (Verification Using a Notary at VVSC whereby VVSC downloads document), Applicant refers to paragraph 72 through 84 and paragraphs 88 through 93, of the original specification.

With respect to FIG 2B (Signature Verification Using a Notary at VVSC whereby VVSC uploads document), Applicant refers to paragraph 72 through 84 and paragraphs 88 through 93, of the original specification.

With respect to FIG 3-3A (Verification Using VVSC Website), Applicant refers to paragraph 72 through 84 and paragraphs 88 through 93, and paragraphs 96-106 of the original specification.

With respect to FIG 3B-3D (Verification Using VVSC Website Whereby a Notary is Required), Applicant refers to paragraph 72 through 84 and paragraphs 88 through 93, and paragraphs 96-106 of the original specification.

With respect to FIG 3D (Identification Criteria), Applicant refers to paragraph 76 through 79, and paragraph 91, and paragraph 93 of the original specification.

With respect to FIG 3E (Client Registration), Applicant refers to paragraph 96 through 98 of the original specification.

APPLICANT RESPONSE TO THE FIRST OFFICE ACTION

In regards to the substantive arguments presented by Examiner, Applicant reiterates its arguments as put forth in the response to the First Office Action, as put forth below.

CLAIM OBJECTIONS

CLAIM AMENDMENTS TO CORRECT INFORMALITIES

Applicant addresses Examiner's concerns regarding claim informalities as put forth in pages 3 through 4 of the first Office Action response. Applicant hereby amends the pending application to correct the following informalities:

With reference to paragraph 5, page 3, Examiner objects to claims 1, 24, and 51 because said claims teach to a method and a system upon which that method is performed. Applicant has amended claims 1, 24, and 51 to teach only the claimed method.

With reference to paragraph 6, page 3, Examiner objects to claims 1, 6, 24, 29, 51 and 57 because the documents produced by the method defined in the specification are possibly not tangible. Applicant agrees with the Examiner's objection and has amended the specification, and the claims, to remove the property of intangibility of the documents.

Application Number 09/973, 273

With reference to paragraph 7, page 4, Examiner objects to claims 1, 24, and 51 because in to next to last limitation of each claim, the host computer server uploads a document to itself. Applicant has amended the claims to define the host computer server uploading a document to the VVSC.

With reference to paragraph 8, page 4, Examiner objects to claim 26 because it claims "the method of claim 24 of claim 24'. Applicant has amended the claim to read "the method of claim 24".

CLAIM REJECTIONS UNDER 35 U.S.C. § 101 and § 112

Applicant notes Examiner's objections with respect to 35 U.S.C. § 101 and § 112.

With reference to paragraph 9, page 5, Examiner objects to claims 9, 32, and 60 as being incomplete under 35 U.S.C. § 112 for omitting essential steps; namely, the method whereby personal genetic information is reduced to genetic code. Applicant agrees with the Examiner and has amended claims 9, 32 and 60.

With reference to paragraph 10, pages 5-6, Examiner objects to claims 7, 8, 31, 58 and 59 as being indefinite under 35 U.S.C. § 112.

Regarding claims 7 and 58, applicant elects to cancel claims 7 and 58.

Application Number 09/973, 273

Regarding claims 8, 31 and 59, Applicant has amended the claims, deleting the term "including", and specifying that the claims teach to claim 8.

With reference to paragraph 11, page 6, Examiner objects to claims 7 and 58 because the claimed use fails to set forth the steps in the process. As noted above, Applicant elects to cancel claims 7 and 58.

Applicant respectfully submits that the amended claims (appended hereto) address the foregoing noted informalities raised pursuant to U.S.C. § 112. Applicant further submits the claims, as amended, are in condition for allowance, and respectfully requests that the Examiner's objections be withdrawn.

CLAIM REJECTIONS UNDER 35 U.S.C. § 103

OBVIOUSNESS

Examiner has rejected claims 1-77 of the pending application as being unpatentable over US Application 2001/0002485 (hereinafter referred to as "Bisbee")[2] in view of US Patent 5,712,914 (hereinafter referred to as "Aucsmith") further in view of US Patent No. 6, 317,777 (hereinafter referred to as "Skarbo").

---

[2] Applicant respectfully submits that the Examiner's arguments may have been rendered moot with respect to the Bisbee application; said application was issued a final rejection by the USPTO on 3/21/2005. Applicant notes that a RCE was filed with the USPTO on 7/13/2005 .

Application Number 09/973, 273

Applicant respectfully submits that Examiner's position is traversed in lieu of an analysis of the application at hand and the prior art. To this end, Applicant submits a substitute specification that discloses the method of the pending application with clarity. Applicant respectfully requests that the Examiner reconsider the 35 U.S.C. §103 objection in accordance with the substitute specification, replacement drawings, and the arguments put forth below.

Applicant wishes to address the substantive arguments put forth by the Examiner under 35 U.S.C. § 103 on the basis of obviousness; addressing the Examiner's objections in turn as put forth in the first office response.

U.S.C.§ 103 ANALYSIS

Examiner submits that claims 1-77 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bisbee (US Patent Application Publication 2001/0002485), in view of Aucsmith in further view of Skarbo et al.

With reference to paragraph 12, lines 4-13, pages 6-7, Examiner cites the prior art of Bisbee as disclosing

> "...a system wherein a set of parties in a networked
> architecture, using Transfer Agents, use a server, a
> Document Authentication System (DAS), in conjunction
> with a notary, called a TCU. Electronic documents are
> transmitted to the TCU via a communication means.... The
> Transfer Agent relays to the TCU a set of verification data,

including digitized hand-written signatures, biometric

information, and a digital signature (certificate), which have

been acquired by a transfer agent from the appropriate

means.

Upon verification of the information provided by the transfer

agent, the TCU appends a certificate to the document to

confirm authenticity, but does not append the biometric

data, or certificates supplied by the transfer agents."

[Emphasis mine].

Applicant notes paragraphs 69-70 of Bisbee which read:

[0069] The information object is digitally signed and/or

encrypted and the authentication certificate is appended by

the DAS, thereby attesting to the fact that the Transfer

Agent witnessed the participants sign the electronic

document. The digitally signed and/or encrypted document

may be electronically communicated to the TCU via a

modem or computer network block 112). Other ways of

communicating digitally signed or encrypted documents

might be used (for example, dispatching a diskette

containing the document), but the great advantage of

electronic communication is speed. [Emphasis mine]

[0070] In addition, although it is currently believed to be preferable for the Transfer Agent to digitally sign an information object before submitting the result to a TCU, it is only necessary for the Transfer Agent to "sign" an information object in a way that can be understood, legally or otherwise, as the Transfer Agent's attesting to the integrity and validity of the information object. For example, the Transfer Agent might append to an information object a digitized hand-written signature, a digitized signature and verifiable biometric information, a digital signature, or a combination of these. Alternatively, the Transfer Agent can sign an information object by connecting to a TCU using the password and other procedures of a secure protocol, such as the secure sockets layer (SSL) security protocol for the TCP/IP (Internet) communication protocol. As should be clear from this description, it is important for the DAS to assure itself that a Transfer Agent is who the Agent purports to be. If not already provided in the course of signing an object, the Transfer Agent appends a hash, a cyclic redundancy check (CRC) information element, or other type of content integrity block to the object, thereby

ensuring the integrity, i.e., unchangeability, of the

information object. [Emphasis mine]

Applicant respectfully traverses for the reasons addressed below.

Bisbee does not disclose the authentication of an identity, or a signature, or a document using a videoconference.

Bisbee does not disclose a method of authenticating an individual or a signature or a document <u>person to person</u>. Bisbee discloses a method and system of using a transfer agent to witness the input of a digital signature; said transfer agent then relays the document to a third party through email or other means.

Bisbee does not disclose a method whereby the signatory to a document is authenticated by any other process than PKI. Rather, Bisbee discloses a method that <u>authenticates that a document originated from a signatory (transfer agent), by using cryptography to identify the sender (transfer agent) of the document and cryptography to identify signed information objects within the document.</u>

Bisbee does not disclose the use of a notary public to authenticate an identity, or a signature, or a document. The method of Bisbee is limited to the use of a

transfer agent who inputs a digital signature after witnessing data input into a document.

Bisbee does not disclose a method whereby the document to be authenticated by the authenticator (TCU) is created by the authenticator.

Paragraph 0028 of Bisbee states:

[0028] ... there is provided a method of handling stored e-original objects that have been created by signing information objects by respective Transfer Agents, submitting signed information objects to a TCU, validating the submitted signed information objects by at least testing the integrity of the contents of each signed information object and the validity of the signature of the respective Transfer Agent, and applying to each validated information object a date-time stamp and a digital signature and authentication certificate of the TCU. The method includes the steps selecting a stored e-original object; re-validating the selected e-original object by at least verifying the digital signature of the TCU applied to the selected e-original object; and applying to the re-validated e-original object a current date-time stamp and a digital signature and current authentication certificate of the TCU. [Emphasis mine]

The method of the pending application discloses a person to person authentication, using a videoconference. Bisbee discloses a method and system of authenticating that a document originated from a signatory; using cryptography to identify the sender (Transfer Agent) of the document.

Examiner states that Bisbee discloses a method of using a notary as a means to authenticate a document (line 1, page 7). Applicant respectfully traverses. Bisbee does not use a notary public as a means of authentication of an individual, a signature, or a document.

In fact , Bisbee is silent on the use of a "notary" as a means of authentication. Upon review of the Bisbee application, one will not find the term notary used as a means of authentication in the specification. In fact, Bisbee cites it's system and method as a substitute for document authentication when a notary public is not available.

Paragraph 0003 of Bisbee states:

> [0003] The continuing evolution of the methods of
>
> commerce is evident in the increasing replacement of
>
> paper-based communications with electronic
>
> communications. When communication is by electronically

reproduced messages such as e-mail, facsimile machine, imaging, electronic data interchange or electronic fund transfer, however, there no longer exists a signature or seal to authenticate the identity of a party to a deal or transaction. <u>The traditional legally accepted methods of verifying the identity of a document's originator, such as physical presence or appearance, a blue-ink signature, personal witness or Notary Public acknowledgment, are not possible.</u> [Emphasis mine]

The Bisbee application further states in paragraph 0004:

[0004] To address these problems, a document authentication system (DAS) has been described that provides the needed security and protection of electronic information objects, or electronic documents and other information objects, and <u>that advantageously utilizes an asymmetric cryptographic system to help ensure that a party originating an information object is electronically identifiable as such.</u> .... [Emphasis mine]

The Bisbee patent fails to disclose the use of a "notary", as traditionally understood in the legal sense of the word[3]:

> Notary publics:
>
> Etymology: Middle English notary clerk, notary public, from
>
> Latin notarius clerk, secretary, from noatarius of shorthand,
>
> from nota note, shorthand character.
>
> : <u>a public officer who attests or certifies writings (as a deed)</u>
>
> <u>to make them authentic and takes affidavits, depositions,</u>
>
> <u>and protests of negotiable paper—called also notary</u>.

As paragraphs 3-4 of Bisbee depict, the method of Bisbee is to <u>authenticate an</u> <u>electronic identity of an document when a notary is not available, using</u> <u>asymmetric cryptographic system as a means of authentication of a document</u>. Bisbee fails to disclose any method, process, or system of notarization.

Bisbee fails to disclose a method whereby the third party authenticator (TCU) creates and issues the document being authenticated. Bisbee is premised on a transfer agent who witnesses a transaction whereby a document is digitally signed. The method of Bisbee teaches that the transfer agent conveys the document to the TCU. The <u>TCU is not the originator of the document to be</u>

---

[3] Merriam Webster Online Dictionary (http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=notary+public&x=17&y=11)

authenticated. The TCU is the recipient of the document of the document to be authenticated and functions as an after the fact authoritative custodian.

Paragraphs 0072-0073 of Bisbee disclose:

[0072] The TCU validates the Transfer Agent's identity and rights and verifies the integrity of submitted information objects. Use of digital signatures directly supports validation of both Transfer Agent identity and information object content integrity. Once it is determined that an information object has not been altered prior to or during submission and that the object's Transfer Agent has the proper authorizations, the TCU assumes custody and control of the object and responsibility for the object's preservation by appending a date-time stamp and digitally signing the submission. [Emphasis mine]

[0073] On receiving a digitally signed electronic object (block 114), the TCU tests the integrity of the electronic object's contents, the validity period of the Transfer Agent's certificate, and the status (valid or revoked) of the authentication certificate (e.g., ITU X.509v3 certificate(s)). The test of the integrity of the object contents, which may also be called "digital signature verification", comprises

<u>extracting the public key from the authentication certificate, decrypting the digital signature (thereby uncovering the object's hash), computing a new object hash, and checking the uncovered hash against the new hash.</u> The test of the validity period comprises simply ensuring that the current date and time falls within the validity period noted in the certificate. The test of the validity of the certificate comprises querying the PKI to determine whether the certificate was not revoked or otherwise restricted at the time of digital signing. <u>These three tests together may be called a "validation" process. Successful tests signify the authenticity of the received digitally signed electronic object, that is to say, who submitted the electronic object and that the object's contents have not changed during the submission process.</u> [Emphasis mine]

The method of the present invention discloses that the third party authenticator (VVSC) <u>creates and issues the document being authenticated, real-time</u>. The method of Bisbee teaches that the transfer agent conveys the document to the TCU. The <u>TCU is not the originator of the document to be authenticated</u>. Likewise, there exists a serious lapse in the chain of custody of the document being authenticated.

Applicant submits that Bisbee fails to disclose a method whereby an identity or a signature or a document is authenticated during a real-time, live-stream videoconference, person to person. As such, Applicant submits that its method is not anticipated by Bisbee and is patentable over Bisbee.

Applicant submits that Bisbee fails to disclose a method whereby an identity or a signature or a document is authenticated during a real-time, live-stream videoconference using a notary public. As such, Applicant submits that its method is not anticipated by Bisbee is patentable over Bisbee.

Applicant submits that Bisbee fails to disclose a method whereby an identity or a signature or a document is authenticated during a real-time, live-stream videoconference, and whereby the authoritative document is created real-time.

As such, Applicant submits that its method is not anticipated by Bisbee is patentable over Bisbee.

Applicant submits that Bisbee fails to disclose a method whereby an identity or a signature or a document is authenticated during a real-time, live-stream videoconference and whereby the authoritative document is issued real-time. As such, Applicant submits that its method is not anticipated by Bisbee is patentable over Bisbee.

Applicant submits that with respect to Skarbo, the Examiner's objection be reconsidered in lieu of the foregoing analysis of Bisbee. Applicant further

submits that Skarbo fails to disclose a method of identity, or signature, or document <u>authentication</u>. Skarbo discloses a method of document collaboration.

DEPENDENT CLAIM OBJECTIONS

Applicant respectfully submits that the foregoing arguments with respect to independent claims 1, 24 and 51 establish sufficient basis for the objections to be withdrawn and that the dependent claims be allowed (with the exception of the claims canceled by Applicant).

In reference to claims 2-23, these claims depend from independent claim 1, which Applicant believes to be allowable in view of the arguments above. As such, applicant submits that claims 2-23 are allowable by virtue of their dependence from claim 1.

In reference to claims 25-50, these claims depend from independent claim 24, which Applicant believes to be allowable in view of the arguments above. As such, applicant submits that claims 25-50 are allowable by virtue of their dependence from claim 24.

In reference to claims 52-77, these claims depend from it independent claim 51, which Applicant believes to be allowable in view of the arguments above. As such, applicant submits that claims 52-77 are allowable by virtue of their dependence from claim 51.

OTHER CITED REFERENCES

The Examiner also cited other references on PTO form 892 but did not use these references in objection the claims. Applicant submits that because these references were not used to reject the claims, the additional references do not teach method of the pending application.

CONCLUSION

Applicant submits that the stated grounds of rejection in the pending claims have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider and withdraw the presently outstanding rejections. It is believed that a full and complete response has been made to the outstanding office action, and as such, the amended application is in condition for allowance. Thus, prompt and favorable consideration of this amendment is respectfully requested. If the Examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at 310-739-9996 or 310-665-0111.
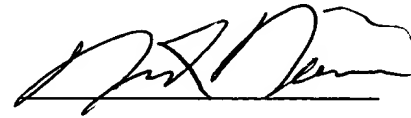
Respectfully Submitted,

Nick Nassiri (Applicant/Inventor)

Application Number 09/973, 273

DECLARATION

Applicant hereby submits a substitute specification, and replacement drawings and declares under oath stating that neither the substitute specification or replacement drawings contain any matter not included in the original specification or drawings.

Nick Nassiri (Applicant/Inventor)